Study: 40% of mobile clicks are accidental or fraudulent

An analysis into the effectiveness of mobile ad spend, and a discussion on click fraud techniques, symptoms and solutions

TRADEMOB

The distribution of useless clicks

Mobile is booming, and so are mobile advertising budgets. However, due to mobile click fraud and the high rate of accidental clicks, only very highly targeted ads can effectively reach the target audience and achieve a profitable ROI. To realise the full potential and possibilities within this new marketing channel, a sophisticated mobile ad verification system is needed.

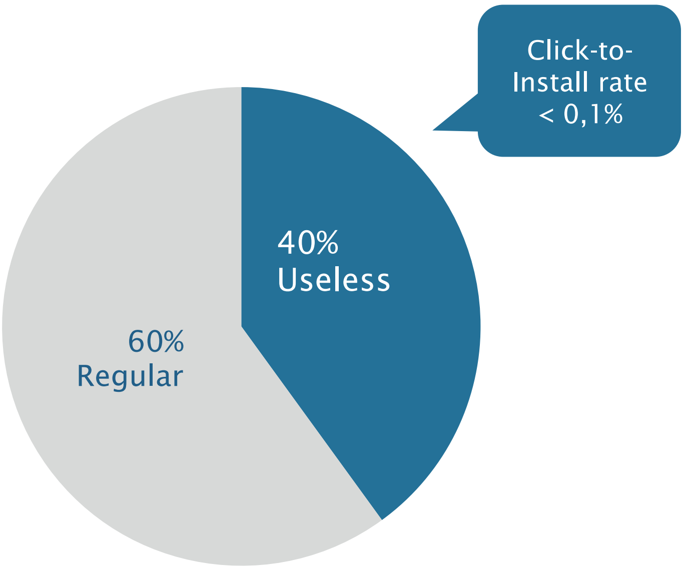
It‘s clear from recent media discussion that clicks need to be monitored in order to ensure that ad spend is used wisely rather than wasted.[1] However, with a noticeable drought of actual studies into the extent of mobile click fraud and the effectiveness of mobile ad spend, Trademob decided to shed some light on the situation.

An analysis of six million mobile ad clicks served across ten different ad networks found that an alarming 40% of bought mobile clicks were worthless, i.e. the conversion rate of clicks to installs was less than 0.1%.[2]

Since the Pay Per Click model takes centre stage as the most prominent reward system offered by most mobile ad networks, these worthless clicks cost companies 40% of their mobile advertising budgets.

40% of all mobile clicks show a conversion rate of <0.1%.

Click category based on after-click conversion rates.



So how can mobile advertisers become invincible to ineffective clicks?

[1] Shalom Berkowitz. (2012, July 3). ‚4 ways to identify mobile click fraud‘. iMedia Connection. Retrieved from http://imediaconnection.com/content/32195.asp

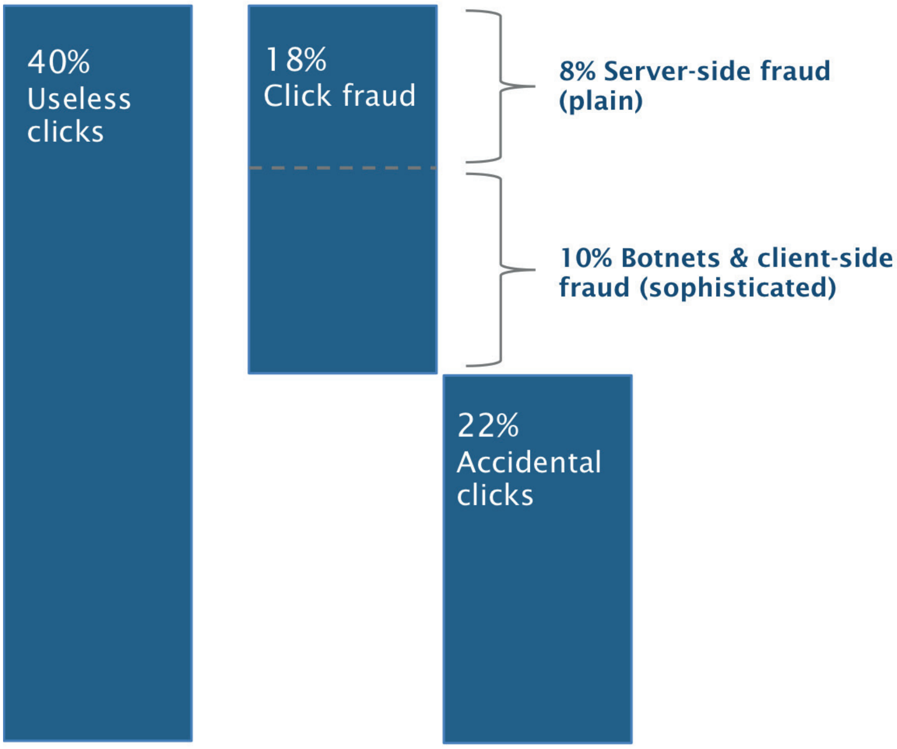
[2] Trademob mobile click fraud study (2012, June)

Mobile click fraud or accidental clicks?

First, let‘s look at where these useless clicks come from. A closer look at the data shows that of this 40%, around half show patterns that are highly symptomatic of click fraud, such as irregular traffic peaks and clicks coming from similar IP addresses, and the others appear to be accidental clicks.[3]

Click fraud and accidental clicks are seriously harming ROI.

Sources of useless mobile ad clicks



Currently, there are three major fraud techniques being used.

Facts of study	
Sample size	6 Million mobile ad clicks
Spread	10 mobile ad networks
Conducted by	Trademob GmbH
Time of data collection	June 2012

The good news?

With the right strategy both sources can be eliminated and the 40% of ineffective ad spend can be saved.

[3] Trademob mobile click fraud study (2012, June)

Accidental clicks

Accidental clicks happen
when a user clicks on an ad by mistake.

This can be due to bad placement, a slip of the hand, or poorly designed, misguiding mobile banners. These useless clicks cannot be associated with click fraud because genuinely accidental clicks do happen sometimes, especially owing to small mobile screen sizes.

In 2011, a study by Pontiflex (Harrison) found that 47% of all mobile clicks happened accidentally.[4] Since then the mobile industry has grown exponentially, smartphone and tablet screens have increased in size, and user behaviour has shifted. Despite an observed decrease, 22% of clicks still happen accidentally and fail to convert.

The solution to this problem is identifying and blacklisting publisher apps and other mobile traffic sources that, purposely or otherwise, create multiple worthless clicks. There‘s just one problem here: in order to make informed choices about publishers, pre- and after-click data need to be matched and analysed, bringing us back to the perpetual dilemma of thorough campaign tracking on iOS.

However, with ad verification techniques and new innovative tracking solutions such as accurate fingerprinting, effective UDID- independent campaign tracking and media buy optimization are possible.

Accidental clicks are really not a new issue in the mobile industry and could be eradicated if ad networks had the right tracking at hand. Still, advertisers lose almost half of their budgets to ineffective clicks.

Clearly, equally as important as advanced tracking is publisher-independency and complete objectivity. Thus, advertisers should rely on unbiased parties having access to the necessary tracking data to optimize their ad spend.

Objectivity and advanced tracking are equally important in detecting accidental clicks.

[4] David Kaplan. (2011, January 27). ‚Pontiflex: About Half Of Mobile App Clicks Are Accidental. paidContent. Retrieved from http://paidcontent.org/2011/01/27/419-pontiflex-about-half-of- mobile-app-clicks-are-accidental/

Mobile click fraud

Click fraud refers to
premeditated clicks that are not driven by a genuine interest in the target of the ad link.

A constant battle exists between fraud and anti- fraud due to both communities continually improving their strategies.

There are difficulties in officially defining click fraud due to the possibility of unethical parties discovering loopholes in the legislation. This however does little to protect advertisers, who are thus unable to dispute or verify reasons for click charges.

A common understanding of click fraud is as follows: by arranging false clicks on ads, shady publishers take advantage of Pay Per Click agreements and charge for clicks with extremely low conversion rates. Performed effectively, this can significantly affect advertising costs and revenue potential.

Click fraud has been an issue for online advertisers since the internet‘s formative years and has already been used by publishers to unfairly deprive advertisers of millions of dollars. As a reaction to better fraud-detection solutions, more cunning and sophisticated fraud systems are conceived, leading to a constant battle between the fraud and anti-fraud communities.

The recent mobile boom means more substantial investment in mobile ads. Global mobile advertising spend was 5.3 billion USD in 2011[5] and is predicted to rise to 24 billion by 2016.[6] With this in mind, it‘s unsurprising that more and more click fraudsters are now targeting mobile ads as well.

So how exactly do fraudsters fill their pockets with the mobile advertiser‘s money?

Mobile click fraudsters haven‘t reinvented the wheel. They mostly rely on traditional online fraud techniques and have more or less successfully adjusted them to the new ecosystem. Three major fraud techniques, comprised of plain and pure server-side fraud, and more sophisticated types (namely botnets and client-side fraud) can be observed. Fortunately, all types can be detected and eliminated with the right expertise and tracking.

[5] Mobile Advertising Market Valued at $5.3 Billion (€3.8 Billion) in 2011‘. (2012, June 6) Interactive Advertising Bureau. Retrived from http://www.iab.net/about_the_iab/ recent_press_releases/press_release_archive/press_release/pr-060612_global

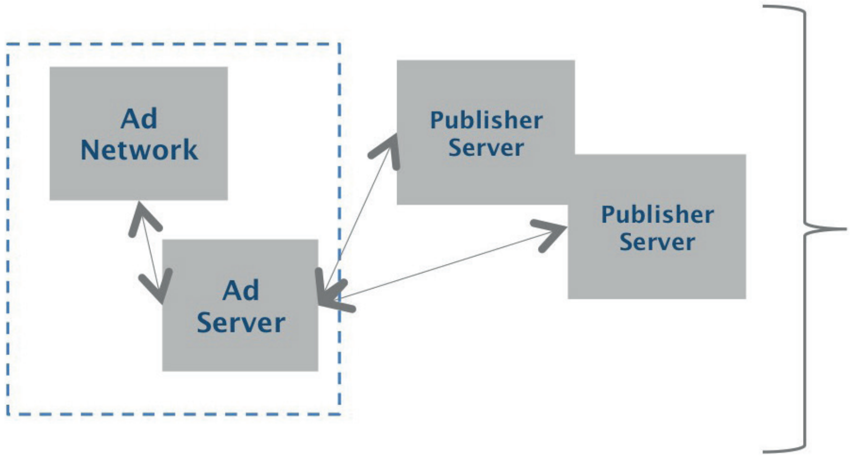
[6] By 2016, Mobile Advertising Outlay Will Equal Current Total Online Ad Spending.‘ (2011, June 23). ABI Research. Retrieved from http://www.abiresearch.com/press/3706-By+2016,+Mobile+Advertising+Outlay+Will+Equal+Current+Total+Online+Ad+Spending

Major mobile click fraud techniques

Plain fraud

Server-side

Publishers use (their own or hacked) servers to report millions of fake clicks per minute, none of which ever actually happened. Though made to look real by sending convincing data, these false clicks are easy to detect with the right tracking solution.

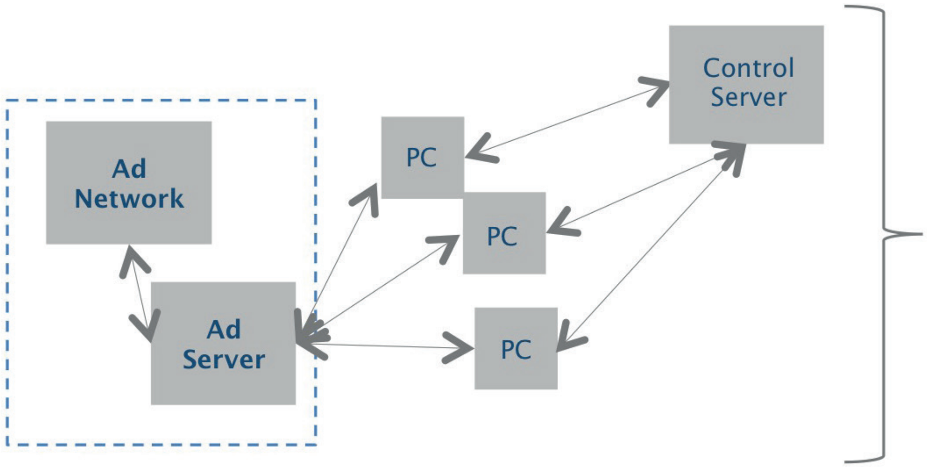


Fake click triggered on publisher server(s)

Sophisticated fraud

Botnets

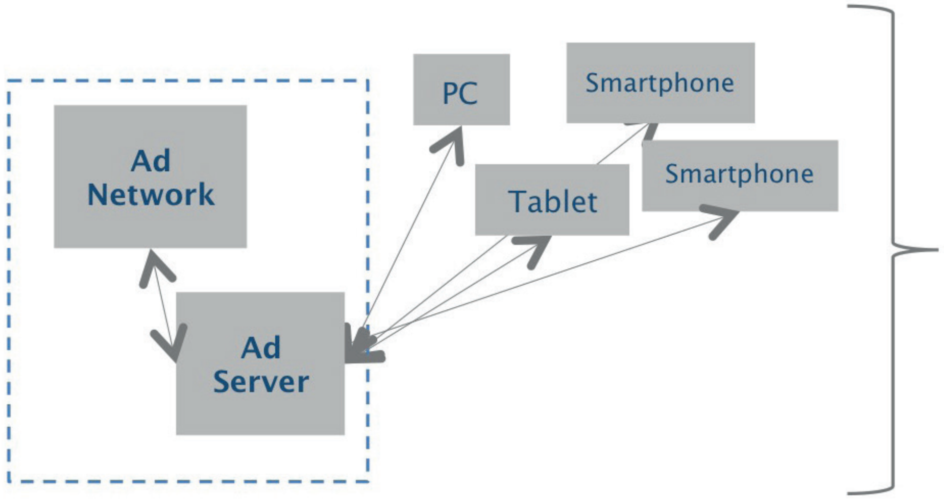
Botnets are inventories of hijacked devices on which viruses are installed, creating fake clicks which go unnoticed by the user due to not being shown onscreen. Most botnets rely on non-mobile inventory but fraudsters can manipulate click-data to appear to be mobile ad clicks.



Click autonomously triggered on hijacked device

Client-side

Unlike plain fraud and botnets, client-side fraud involves actual user interaction. This again goes unobserved by the user. By way of example, a person might unintentionally click on an ad banner which is hidden behind another banner, with the publisher then charging the ad network for both the intentional and unintentional clicks.



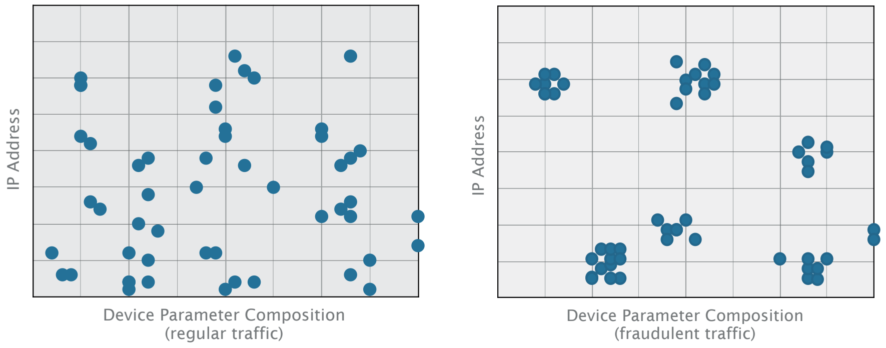
Click (in)-directly triggered by user

The bright side: detection of click fraud

Detecting plain fraud

Server-side fraud is probably the most basic form of click fraud and is relatively easy to detect. As clicks are sent from the same server(s), they come from the same IP address and the header data which are transferred along with each click will show a similar device parameter composition, also referred to as fingerprint. With the right tracking and algorithm, these bulks of clicks sharing the same IP address and parameter composition can quickly be identified.

Click bulks of IP address and fingerprints can uncover plain fraud.

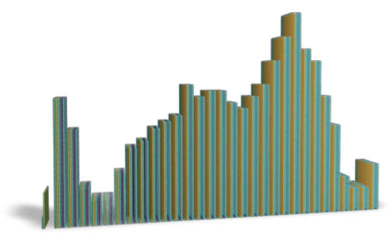


Detecting sophisticated fraud

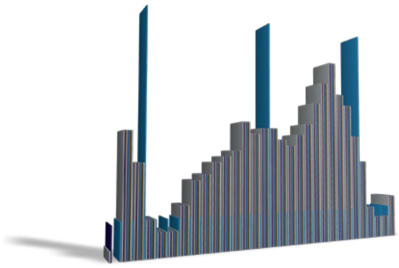
The more sophisticated fraudsters have established their own ‘inventory management’ to increase the IP distribution and optimize click reporting to conceal fraud the best way possible. However, these days, most mobile fraudsters only apply the minimum effort required in order to achieve their goals, and these cover-up strategies are still immature.

Deeper analysis of click data by ad verification platforms can therefore also reveal more advanced types of fraud. We may still see peaks of clicks at unexpected times of day, for example.

Under investigation, fraud is found out through **inconsistent activity** and **irregular patterns**.



Daily click pattern reported by publishers

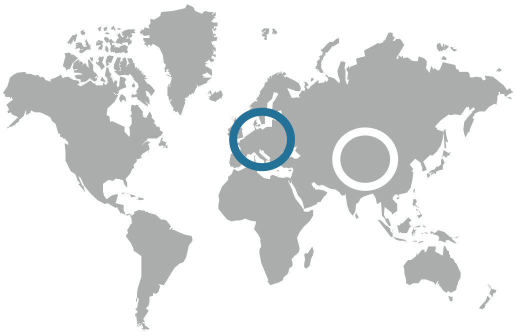


Daily click pattern with irregular peaks (reported by shady publishers)

But the biggest hurdle for shady publishers is that they don’t know the campaign settings, so the click data may not match the selected target.

Let’s say a mobile ad campaign is targeted to be shown only to iPhone users located in Western Europe. A fraudster, noticing a high-paying CPC click on his mobile website executed by a German user, decides to increase his revenue stream using his ‘botnet’ made up of hijacked Android phones in India to report more of these well-paying clicks. Tracking reveals these discrepancies.

Fraudsters don‘t know campaign settings such as target area.



Fraudsters report clicks from outside the target zone

Optimizing ROI through ad verification

Summary

Click fraud and accidental clicks could cost advertisers as much as 40% of their advertising budget, money which is far better spent where it has a positive impact. Fortunately, this 40% can be moved back into an advertiser's efficient ad spend and help ensure the effectiveness of their mobile ad campaigns.

In order to optimize a mobile ad campaign, it is vital to use ad verification to spot and blacklist sources of click fraud and accidental clicks who cost money but offer nothing in return. By tracking ad campaigns and analysing pre- and after-click data, it is possible to sink publishers that underperform and invest in the ones that bring revenue. Such a cross-network blacklisting of useless publishers requires a deep integration with ad networks, access to publisher and user data and an advanced tracking technology that can create a unique fingerprint for each click source and match clicks with after-click actions.

With **advanced tracking** and **ad verification,** useless clicks can be stamped out.

Choosing the right strategy

Besides sophisticated tracking data, an independent and objective optimization is required to ensure that mobile ad spend is allocated to its most effective sources.

It's possible to invest only in publishers that bring in app users and ROI. Via advanced fingerprint technology, thorough optimization and an objective approach, accidental clicks and fraud can be detected and prevented.

While advertisers are obviously pure in their intentions to maximize their ROI, they lack the tracking technologies as well as access to the click- and publisher data. Even with the desired data at hand, analysing and preventing ineffective clicks requires automated systems, a deep technical network-integration and the right algorithm. Advertisers will thus most likely face huge manual effort here, without achieving the desired results. On the other hand, many ad networks lack the sophisticated tracking solution and data. And given that they are caught between three business goals (the advertiser's satisfaction, the publisher's satisfaction and their own revenue stream), campaign optimization is, by nature, corrupted. Advertisers thus depend on objective intermediaries advocating their interests.

What can Trademob do?

As an aggregation platform, Trademob is able to focus on advertisers' interests whilst remaining independent from publishers. Providing accurate and proven fingerprint tracking, a close collaboration with ad networks and a clear optimization focus, we ensure that our clients' marketing goals are achieved in the best, most efficient way. As a result, transparent and revenue-driving campaigns make mobile advertising profitable for the advertiser and mobile marketing budgets rise. Advertisers, ad networks and trustworthy publishers all benefit from our advertiser-targeted solution.

A 100% **advertiser-targeted solution** enables true campaign optimization.

Disclosing and blacklisting click fraud and accidental clicks can eradicate 40% of ineffective mobile ad spend and ramp-up ROI. However, there are many more optimization settings such as; banner type, timing, device, channel, and location. Therefore it comes as little surprise that we see overall optimization for our clients' targeted mobile advertising campaigns as high as 70%.

Advanced campaign optimization sees an ROI increase of up to 70%.

Appendix:
Mobile click fraud techniques in more technical detail

As we've only scratched the surface of mobile click fraud types in the previous section, here's a more detailed account for those of you harbouring a hidden passion for IT.

Server-side click fraud

Historically, fraud originated from single machines like privately owned PCs and servers, with increased professionalism progressing into server clusters and cloud-hosters. As the number of machines is a limiting factor, each machine needs to deliver a good number of fraudulent requests, ideally clicks and impressions, to generate an unsuspicious clickthrough rate.

Current mobile fraud attempts are still largely very primitive.

The generation of the necessary partly-forged http-requests is carried out by scripts or full-blown fraud-suites obtainable on the internet's black market. The most sophisticated come with a throttling of requests to avoid 'off-the-chart' effects that could trigger a review and also a multitude of faked browser-headers to show a good distribution of users.

But even with the increase of hacked servers, this source of fraud can easily be detected. The limit in server numbers means a tight clustering of IP addresses as well as fingerprinting parameters. Also with different tools and scripts in use by the fraudster, each cluster can show a specific distribution of client-parameters.

In addition to the shown weaknesses in masking their unwanted behaviour, javascript and other more complex client-side technologies are often ignored in simple fraud attempts. This might be due to the fact that per server performance and tight control over http-behaviour is a dominant requirement for server-side fraud.

Botnets

When single servers are not available or too easy to blacklist, a cheap and willing workforce of hacked consumer PCs is available to paying 'customers'. Botnets, when perceived as a platform, can be utilised for online and mobile fraud with a similar toolset as for server-side fraud.

The renting is flexible, fees are low and the IP distribution is drastically increased, though it still depends on the size and quality of the used network. Due to the volatile nature of clients caught in a botnet, detection and blacklisting can be harder to achieve by opposing ad-networks or DSPs.

Botnet owners have developed an own 'inventory management' of their hijacked devices to cover up their unethical activities.

Client-side

With the recent sharp increase right at the zenith of Web 2.0, client-side technology has become the new playground for script- kiddies, benevolent hackers and clever fraudsters alike. Somewhat tech-savvy webmasters with a significant user base may think their mobile page needs a bump in revenue. They can be tempted, once they realise how easy it is, to place banners inside invisible layers and put paying clicks on close buttons or fake scrollbars. Due to the diversity in users on international sites this kind of fraud will be harder to detect as long as they are able to slip through the ad network's quality controls.

It gets much more complex when fraudsters decide to parasite on other sites, using cross-site scripting and SQL-injects as their most common angles of attack. This approach programs legitimate websites to serve malicious javascript code which in turn makes the unaware user generate visible or invisible clicks on high CPC- campaigns. All of this is configured and frequency-capped by the fraudster's 'inventory management' on yet another hijacked machine.

Client-side fraud techniques show the highest diversity of IPs and device parameters, leaving fewer other data to identify a pattern. Some publishers also decide to 'charge' their real clicks by a humble factor of 2 to 10, showing at least some conversions in performance reports. With this in mind, it is evident that there is a clear need for a scientific approach and number crunching on past experience to detect fraud when it comes to its advanced stages.

Close collaboration of the anti-fraud community can affront more sophisticated fraud in the future.

Conclusion

Though click fraud might sound sophisticated, in reality fraudsters currently only apply the minimum effort required to achieve their goals. Right now there is only very little creativity needed to overcome basic macro-plausibility checks and much of their work goes undetected. Simple fraud techniques still work out in a big way – an arms race between the fraud and anti-fraud side has yet to be triggered. On the bright side, it means that platforms with access to both pre-and after-click data, can quickly expose fraudulent publishers.

Looking ahead, it is likely that fraudsters will change strategies when a major part of the market is able to detect their activity. So fraud detection and prevention will likely be challenged in the future and will require a close collaboration among the anti-fraud community, with cross-network and cross-campaign tracking and data analysis forming the initial steps.

Questions?
Ask us.

TRADEMOB

The Data-Driven App Marketing Platform

Global, Independent, Transparent
Mobile Advertising for your App.

info@trademob.com, www.trademob.com
Berlin, London, Paris, Madrid, New York